CRS Build 10.0/VIP Build 3.1 Release Notes

These notes document the new features and bug fixes incorporated into the CRS Build 10.0 and VIP Build 3.1 software releases. Engineering Change Request (TTR) numbers have been provided to reference a formally documented problem which has been resolved by this build. The following TTRs are listed numerically in two categories: New software enhancements/capabilities and bug fixes.

SOFTWARE ENHANCEMENTS

1. **TTR 832: Support For Externally Generated Voice Messages - THIS FEATURE WILL NOT BE ACTIVATED IN BUILD 10.0. IF CRS BUILD 10.0 RECEIVES AN EXTERNALLY GENERATED VOICE MESSAGE, AN ALERT MONITOR ERROR MESSAGE WILL BE GENERATED AND THE MESSAGE WILL BE DELETED. IF THIS CAPABILITY IS NEEDED IN THE FUTURE TO SUPPORT THE ALL HAZARDS COLLECTION SYTEM, IT WILL BE ACTIVATED AT THAT TIME.** Prior to Build 10.0, CRS software only received weather related messages in ASCII text format. It processes the messages based on Message Attributes stored in the weather message header and system data stored in various database tables. These text messages are converted from text to speech either using the DECtalk algorithm or using the VIP. Prior to Build 10.0, CRS did not provide the capability for processing externally generated voice messages.

   Build 10.0 provides the capability to process, schedule, and broadcast externally generated voice messages. The CRS weather message header Message Attributes include a 5-character Message Format code used to identify the format and language of the message. Previously, the only Message Formats that could be properly processed were "T_ENG" and "T_SPA" for English and Spanish text respectively. The Build 10.0 software will process "V_ENG" and "V_SPA" for English and Spanish voice. **The CRS formatter generating the voice message and forwarding it to CRS is responsible for ensuring it is properly constructed so that CRS can successfully process it.** Since these voice files will be passed through the DECtalk for broadcast on the transmitter in the same manner as manually recorded voice files, either of the "voice" Message Formats may be used for both English and Spanish externally generated voice files. However, for consistency, we recommend the use of "V_ENG" only for all externally generated voice files.

The following is the format of the message name for the externally generated voice messages:

EV ID <msg typ ID> <msg ID>

where <msg typ ID> is the internally-assigned numeric Message Type identifier and <msg ID> is the internally-assigned numeric message identifier of the subject message.

Some restrictions are required for the proper handling of the externally generated voice files. Because the weather message header must be extracted in its entirety, the **CTRL-F** and **CTRL-B** sequences are **not** permitted to be imbedded in the voice file. The new voice processing software will pass through DECtalk formatted .wav files, i.e. 10K sample .wav files. The software will also recognize and convert using the SOX utility the more standard 16K sample .wav files. All voice files must be monaural.

2. **TTR 831: <u>Add Special DMO Test NWRSAME Capability</u>** - Prior to Build 10.0, CRS did not have the capability to perform the DMO Test NWRSAME. This special event code provides the NWS field offices a means of conducting exercises to practice issuing authentic warnings and other critical messages without disrupting the EAS network or turning on receiver codes used by industry and the general public. It may also be used as a maintenance aid to align and test the communications link.

   The CRS software has been modified to check for special Event Code "DMO". If found, CRS will ignore the normal NWRSAME generation of UGC codes based on the LACs in the message header. Instead, CRS will generate a single code of "999000". The event code "DMO" should not normally be programmed into the receiver decoder, and the location code of "999000" does not match any existing or future geographical area codes.

   Important Note: Even though receiver codes in NWR receivers and EAS equipment are not turned on by the DMO Test Message, the complete message including the NWRSAME tone will be broadcast by the transmitter and received by radios that are already turned on for broadcast monitoring. Therefore, sites generating the DMO Test Message should not generate the 1050 Hz Alert tone and should include appropriate test language in the message.

3. **TTR 804: <u>Replacement Of FTP Transactions With SFTP</u>** - The CRS consists of 2 MPs, 2 -4 FEPs, and a single VIP. CRS receives specially formatted text messages from AWIPS that are placed in a directory on the Master MP for processing. Text messages that are flagged to be transformed into the Speechify voices (Tom, Donna, and Javier) are sent to the VIP for processing. The VIP will convert the text messages to 16K sample .wav files. Optionally these .wav files may be directed through LDAD to external systems, such as Web Servers, the WR Interactive Voice Response (IVR) system, etc. This option also allows for the files to be converted via the SOX utility to mp3 files and transferred. After the files received from the Master MP are processed, the SOX utility is

used to convert them 10K sample .wav files, which is the format required for DECtalk acceptance. The 10K sample .wav files are transferred back to the Master MP, where they are scheduled and copied to the shadow MP and FEPs for subsequent transmission. Control files are also passed back and forth between the Master MP and VIP that allow the transfer of timeout and status information.

Prior to CRS Build 10.0/VIP 3.1, all the message transactions between AWIPS and Master MP, Master MP and VIP, and VIP and external systems were via file transfer protocol (ftp). These ftp transactions require the passing of the crs user password between systems and create security problems that are in violation of the DOC Computer Security Policy. Therefore, these transactions will be replaced with secure file transfer protocol (sftp). The sftp required the passing of authentication keys between the systems rather than a password. Because the transition from ftp to sftp in CRS Build 10.0 requires close coordination of this same change implemented in AWIPS OB4, ftp will remain as an option for transactions between AWIPS and the Master MP. This will allow sites to install either AWIPS OB4 or CRS Build 10.0 first. **LATEST AWIPS UPDATE: PLEASE NOTE THAT BECAUSE OF AWIPS LOADING PROBLEMS, AWIPS OB4 WILL NOT BE IMPLEMENTING SFTP. TRANSACTIONS FROM AWIPS TO CRS WILL CONTINUE TO USE FTP.** However transactions between Master MP and VIP and those between VIP and external systems will only be with sftp. For those functions, the ftp function will be removed in CRS Build 10.0/VIP Build 3.1.

The MPs and VIP support openssh connections between themselves and AWIPS. This allows for the use of sftp, secure shell (ssh), and secure telnet. Authentication keys are needed to authorize these transfers or remote sessions. Public and private key files have been established on all these processors as part of the installation process. The VIP disk recovery procedure continues to be the utilization of CD imaging system to restore the disk. The recovery procedures will include new steps for the authorization keys. Generally, if the CRS application is re-installed, the authorization keys remain intact, and no steps to re-establish the keys are necessary. However, if the CRS application software is being re-installed as the result of an MP hard drive replacement, the keys will need to be re-established. Appendix C, CRS Build Installation Procedure, has been modified to reflect this fact.

Paths: After the initial CRS Build 10.0 software is installed, six or seven connections are defined that support sftp transfers and ssh remote sessions. The six required paths are AWIPS to 0MP, AWIPS to 5MP, 0MP to VIP, 5MP to VIP, VIP to 0MP, and VIP to 5MP. The optional path is VIP to External System.

Key Configuration Files: The sftp transfers and ssh sessions require that openssh has

configuration data. Public key data must be in the files for all the authorized systems that will transfer data to the system under configuration. All the public key data used by the setup scripts will be in three types of files:

1. **Individual Public Data Key Files**: These are mathematical data and the public half of a pair of keys. Each key is associated with the private key at the originating end of the paths described above. These keys are in filenames with extensions of "pub".

2. **Authorized Key Files**: These are an aggregate of the public key data. These are the individual identity key pairs created for a unique user to identify without a password.

3. **Known Hosts Key Files:** These are an aggregate of the public key data. These are the keys used for computer to computer communication during the encryption process.

A system wide file called **Known Hosts File** also exists as part of the system ssh configuration directory. These are the configuration files used directly by openssh and contain several keys.

Key Generation Scripts: Key generation is done with the contents of the public and private mathematical keystring files for openssh encryption. The key generation for 0MP and 5MP is done when they are first rebooted immediately following the installation of Build 10.0. After its initial use, the key generation script is stored on the 0MP in /etc/config/osdone/sshinstaller.sh. The VIP key generation is done in a similar manner. The scripts will not replace key files already generated, but will generate new and distinct files if a key file is absent. If new keys are generated, the key configuration script must be rerun on the MPs and VIP.

Key Configuration Script: This is also called the fixkey script. This script will display a fingerprint of the public key files for verification and concatenate them together into their respective authorized key files. It will then prompt for known hosts fingerprints approval and add the approved host public key information into the known hosts key files.

Fingerprint: This is a short string of hexadecimal digits in ASCII text string format. This check sum of a public key file that can confirm the correct key data is used comparing it to a stored, printed copy of the fingerprint sequence.

4. **TTR 805: <u>CRS And VIP Automatic Password Checking</u>** - Prior to CRS Build 10/VIP Build 3.1, very little automatic password checking was performed.

The following six rules for password checking have been added to the MP, FEP, and VIP

systems for all users except root, switchmp, and sysadm:

a. Password must have at least 8 non-blank characters.

b. Password must contain at least two alphabetic characters.

c. Password must contain at least one number.

d. Password must have at least 3 different characters from the old password.

e. Password must differ from the user name, any circular shift of the user name, reverse order of the user name, or any reverse circular shift of the user name. (Please note that all CRS user accounts contain fewer than 8 characters. Therefore, having the user name as the password will fail on the restriction described above in (a.).

f. Password must be changed at least every 90 days.

Additionally, the following four rules for password checking have been added to the VIP system:

a. Password must contain at least one upper case alphabetic character.

b. Six of the characters may occur only once in the password.

c. In addition to the current password, the password cannot be changed to the 10 previous passwords. Therefore, the current password will not be able to be re-used for the next 11 password changes.

d. Password cannot contain vendor/manufacturer default passwords, words found in any dictionary (forward or backward), addresses, birthdays, or common character sequence.

Additionally, the FEP requires the password contain the two alphabetic characters and one number within the first 8 characters.

Because of password aging, when the operator logs into the CRS GUI or the KDE desktop, a pop-up dialog will display in the upper left-hand corner of the display advising him in how many days the respective password will expire. The operator must click **okay** to continue the login.

IMPORTANT NOTE: PASSWORDS FOR ALL USERS SHOULD BE CHANGED AT THE SAME TIME. THE WARNING AND EXPIRATION MESSAGES WILL ONLY BE SEEN FOR THOSE USERS THAT YOU LOG INTO. FOR

EXAMPLE, MOST SITES DO NOT LOG IN AS CRS USER. THEREFORE, IF THE CRS USER PASSWORD IS GETTING CLOSE TO EXPIRATION OR HAS IN FACT EXPIRED, THE OPERATOR MAY NOT SEE THE WARNING OR EXPIRATION MESSAGE. THEREFORE, SITES SHOULD MAKE SURE THAT WHEN THEY SEE THE PASSWORD WARNING OR EXPIRATION MESSAGE FOR ONE USER, THEY CHANGE PASSWORDS FOR ALL USERS FOLLOWING THE PROCEDURES IN APPENDIX A OF THE DRAFT SYSTEM ADMINISTRATION MANUAL.

5. **TTR 807: VIP Disk Imaging System Changed To Mondo Image System** - Prior to VIP Build 3.1, the VIP operating system and application software distribution, backup, and recovery were performed using a DOS based package called Drive Image from PowerQuest. This disk imaging system was difficult to generate the disk image and very time consuming because it did not directly support the Linux ext3 file systems.

   The new Mondo Image System is an open source Linux based package that has been used previously in other NWS supported Linux systems. It boots to Linux off a CD (Drive Image required a bootable diskette, and was itself run from diskette) and can completely restore the VIP operating system and application to a hard drive. It is Linux based and can more easily handle the ext3 file systems.

6. **TTR 808: CRS Application Changes In MPs To Accommodate SFTP Transactions With VIP** - Prior to CRS Build 10.0, CRS used the ftp.ksh script to used the clear text crs user password for ftp transfer to and from VIP. It also used the chg_emb_pw.ksh script during CRS application install and when passwords were changed to prompt the user to enter the crs user password. The chg_emb_pw script placed this password in the ftp.ksh script and distributed the updated ftp.ksh script to the other processors.

   All references to ftp are changed to sftp. Commands will be accessed from a dynamically created text file using functionality built into the sftp so that the previous ftp mechanism is retained. The clear text crs user password has been removed from the ftp.ksh script. This change also requires the removal of the chg_emb_pw.ksh script.

7. **TTR 809: SFTP Flag Installation On AWIPS** - Prior to CRS Build 10.0, all the message transactions between AWIPS and the Master MP were via ftp.

   Because the transition from ftp to sftp in CRS Build 10.0 requires close coordination of this same change implemented in AWIPS OB4, ftp will remain as an option for transactions between AWIPS and the Master MP. This will allow sites to install either AWIPS OB4 or CRS Build 10.0 first. When sites install CRS Build 10.0, the installation instructions will direct the installer to place a marker file in the a shared directory in the AWIPS system. The AWIPS OB4 software will look for that file to direct it to use sftp for file transfer to CRS. Otherwise, it will continue to use ftp.

LATEST AWIPS UPDATE: PLEASE NOTE THAT BECAUSE OF AWIPS LOADING PROBLEMS, AWIPS OB4 WILL NOT BE IMPLEMENTING SFTP. TRANSACTIONS FROM AWIPS TO CRS WILL CONTINUE TO USE FTP. THEREFORE, THE MARKER FILE WILL NOT BE INSTALLED ON AWIPS.

8. **TTR 811: VIP SFTP Changes** - Prior to VIP Build 3.1, VIP used ftp for all message transactions to and from the CRS Master MP and to external systems (remote ftp).

   Libraries have been added to VIP to support the sftp and ssh protocols. All transactions to and from the CRS Master MP and to external systems (remote ftp) will now use the sftp protocol. For Master MP/VIP transactions this includes receipt of VIP text messages, transmittal of wave files, and receipt/transmittal of status information.

9. **TTR 813: CRS SFTP Wrapper** - Prior to CRS Build 10.0, CRS used ftp for both sending/receiving files to/from other systems. The ftp wrapper used within CRS contains logic that at the end of the ftp session, signals the CP_AI_RCV binary to look in the appropriate Master MP directory for a new raw text message.

   A similar sftp wrapper has been written to check in the appropriate directory at the end of the sftp session.

10. **TTR 815: Expansion Of Civilian Generated Event Codes Table** - CRS Build 8.5 included the capability to generate a SAME originator code for civilian (non-NWS) generated event codes. NWS generated event codes have an originator code of WXR. The civilian generated event codes have an originator code of CIV. Build 8.5 defined a new file on the MPs: /crs/data/SS/SAME_event_codes.dat with the four civilian generated event codes: CEM, EVI, ADR, and CAE.

    The Build 9.0.1 patch distributed in January 2004, added the following 16 additional event codes to the event code table: AVA, AVW, CDW, EQW, FRW, HMW, LEW, LAE, TOE, NUW, RHW, SPW, VOW, NIC, NPT, and NMN.

    Since Build 9.0.1 was implemented as a patch, this writeup is being included in the Build 10.0 Release Notes to ensure that the updated /crs/data/SS/SAME_event_codes.dat file is being included in the ClearCase software build procedure.

BUG FIXES

1. **TTR 833: <u>Date Time/AWIPS Time Updates Stop/Start Message Processing Software</u>** - Date/Time updates and AWIPS time request updates generated by the CRS operator from the CRS Maintenance menu will always stop the CP_VC process, which is responsible for all VIP message processing, which will cause the VIP icon in the status window to go down briefly. This is necessary since CRS system time updates will affect the processing of incoming message effective/expiration time processing. However, the automatic stopping and subsequent starting of the VIP message processing process may prove to be confusing to the operator.

   The Date/Time Update window has been modified to add the following Information Dialog when the operator initiates a time change request:

   Update time will restart VIP interface stop/start cp_vc

   The operator will be given the opportunity to continue with the command or cancel it.

2. **TTR 834: <u>Multiple Future Effective Time Watch/Warning Interrupts Not Scheduled</u>** - Prior to CRS Build 10.0, multiple watch/warning interrupts with effective times in the future were not scheduled. For example, suppose the current time was 2200 and a severe thunderstorm warning (WBCSVRWBC) was received with an effective time of 2210. Then another severe thunderstorm warning (WBCSVRWBC) was received before 2210 with an effective time of 2220. Normally, the second message should replace the first message. However, in this operationally esoteric case, neither the first nor second message would ever play.

   The CRS software has been modified to handle this operational situation in a more reasonable manner. In the example described above, the first message would not play when its effective time was reached. Instead, because its effective time was in the future when it was received, it will be permanently replaced by the second message, thereby ensuring that it will never play. The second message will play when its effective time is reached.

3. **TTR 835: <u>MMI Display's Font Is Too Small</u>** - Prior to CRS Build 10.0, the font used for the Message Monitor (MMI display) was Helvetica 7. Middle Aged eyes found this very difficult to read.

   The font has been changed to Helvetica 10.

4. **TTR 836: <u>CRS/ROAMS Interface Software Does Not Recognize Local 10-Digit Dialing Bit</u>** - Prior to CRS Build 10.0, the CRS/ROAMS interface software in CRS did not recognize the bit used to define local 10-digit dialing. Therefore, the display resulting

from a Query to a ROAMS set for 10-digit dialing would include a garbled area code in the telephone number. For example, a site using 10-digit dialing with an area code of 785 would display an area code of 7185 after the Query.

The CRS software has been modified to check if the area code is overflowed as a result of the 10-digit dialing. If it is overflowed, it will offset the area code to adjust the display properly.

5. **TTR 786: VIP Processing/Manual Recording Collision** - Prior to CRS Build 10.0, it was possible to encounter problems while simultaneously manually recording a Weather Message (either Weather Message record or Emergency Override) and processing a VIP message. This could result in the stopping/starting of CRS. If database problems existed, CRS may not start successfully, which would require operator intervention to clean up the database. As a result, we recommended that sites separate the manual record function from the VIP processing function, i.e. make sure that all manual recordings are made on ACP2 (Shadow Console).

   To distribute both digitized voice (manual voice recordings) and VIP wave files in a manner that alleviates the collision problems, the stream copy client/server logic was rewritten to support two stream copy processes. One supports digitized voice messages, the other supports VIP wave files. The new logic facilitates the stopping of all processing of any VIP message that is being stream copied while a digitized voice message is being distributed.

6. **TTR 806: VIP OS Security Patches** - When the Harris Scan software was performed on the VIP Red Hat Linux Version 7.3, it detected four security deficiencies for which patches exist but had not been installed. These four security patches and all production patch packages available from Red Hat, Red Hat Legacy, and the NOAA NCIRT patch server through May 3, 2004 have been applied to VIP Build 3.1.

7. **TTR 810: Messages With Duplicate LACs Are Not Scheduled** - Prior to CRS Build 10.0, messages containing duplicate Listening Area Codes (LACs) in the Message Attribute Header would result in its failure to be scheduled. Additionally, it would result in the generation of a log entry from CP_VC concerning DB_MH notification failing, the this error message did not go to the Alert Monitor. Therefore, the operator would be left with a situation where a message was not being scheduled, but no operator notification that would indicate what the problem might be.

   The CRS Build 10.0 software includes a new function that performs a duplicate check that is used withing the LAC parser. This check will allow the parser to "skip over" duplicate LACs and process the message normally.

   In the course of testing this change, we discovered that the changed exacerbated an existing, but never before detected problem. If a message incorrectly separates multiple

LACs, i.e. using a "," instead of "-", the new function will cause the software to enter into an infinite loop. This problem has been fixed so the software will properly detect the illegal delimiter.

8. **TTR 812: <u>Remote FTP Script Changes</u>** - Prior to VIP Build 3.1, sometimes the VIPserver would not finish the conversion before the ftp put function called in the remote ftp of MP3 files. Also, the pre-defined length of the remote ftp string (remote username:hostname:password) was not always long enough to support what had to be entered.

   The remote ftp script has been modified to insert a 10-second delay in the script for the remote ftp of MP3 files. The 23 character string limitation has been increased to 32.

9. **TTR 816: <u>Remove Spurious Messages From The MMI</u>** - Prior to CRS Build 10.0, a number of error messages routinely displayed in the MMI, which caused questions and confusion. These errors include the following:

   a. **System not licensed or unregistered software.**

   b. **Multi-line sendmail errors (unqualified hostname 0mp unknown) with retrys.**

   CRS Build 10.0 removes both a and b.

10. **TTR 819: <u>Multiple Sets Of VIPserver Processes May Run</u>** - It is possible for the VIP GUI to stop running, even though the VIPserver processes continue to run. In this case, even though the operator cannot access the VIP control windows, the VIP icon in the CRS Status window is up and VIP messages continue to be processed. The problem is that the natural reaction to this situation is for the operator to restart the GUI. After the GUI is up and operating, the main GUI menu will indicate that VIP is down, **even though it is not.** Therefore, the natural reaction of the operator is to restart the VIP application.

    Now the VIP menu will indicate that VIP is up, and the operator will assume all is O.K. Prior to VIP 3.1, when the operator restarted the VIP application under these circumstances, he was actually starting a second set of VIPserver processes. **When more than one set of VIPserver processes are running, the results of the VIP conversion may be disastrous.** Both sets of VIPserver processes are processing the same message and the results are unpredictable. The converted wave file may have long gaps of silence or may play much too fast.

    Modifications in VIP Build 3.1 have been made that kill all the old VIPserver processes when the VIP application is restarted. This prevents the multiple VIPserver scenario described above.

11. **TTR 821: <u>SOM Changes</u>** - The Operational Build 9.0 version of the CRS Site Operator's Manual (SOM) is missing the Create ASCII file button on all figures depicting the the XCRS_Site Configuration Developer screen (Figures 141, 142, 143, and 144). It also is missing the text that describes the function. Also, Section 3.6.2.5.13 of the SOM, Off-Line Tone Generator, does not have language specifically instructing the user to close the Transmitter Configure window following the disabling of the transmitter and prior to entering the Off-Line Tone Generator window.

    The Operational Build 10.0 version of the SOM has been changed to include modified

    Figures 141 - 144 to depict the additional button, the language describing the button's function, and the language to exit the Transmitter Configure window in the appropriate part of Section 3.6.2.5.13. These changes have also been included in the on-line Hyper Text Help pages.

12. **TTR 823: <u>Some Site Identifiers Are Incorrect In The VIP</u>** - Prior to VIP Build 3.1, the VIP file WFOsites.env had several incorrect entries. This file contains the list of approved sites during delivery of new VIP software. Only site identifiers in this list may be entered during VIP software setup via the Setup Wizard. Once the site identifier is selected, it is written to the version file on the VIP. This file is used during the configuration of the remote ftp. Therefore, an incorrect sited identifier in the WFOsites.env file will contaminate the remote ftp configuration.

    The following lists each site, the old identifier, and the new identifier in VIP Build 3.1:

Site	*Old ID*	*New ID*
Jacksonville, FL	**KJAN**	**KJAX**
Key West, FL	**KEYN**	**KEYW**
NMTW (Alpha)	**NMTW**	**NMTW**
NWSHQ2 (Beta)	**NNHDA**	**NHDA**

    Also, neither the CRS nor VIP Site Identifier file contained the identifiers for the 3 NRC systems. Therefore, CRS Build 10.0 and VIP Build 3.1 will modify the respective files to include the 3 NRC identifiers as follows:

Site	*Old ID*	*New ID*
NRC System 1		**NRC1**
NRC System 2		**NRC2**
NRC System 3		**NRC3**

13. **TTR 803: Off-Line Tone Generator Failure To Write Configuration To Disk** - Prior to Build 10.0, the CRS Off-Line Tone Generator software did not write changes to tone amplitude to the transmitter configuration file stored on the MP hard drive. The changes were correctly made in memory, resulting in the tones being generated with the newly modified amplitude. However, at some later point in time when the CRS application was terminated and then restarted, the tone amplitude written into memory from the configuration file was the old value. Therefore, from that point on the tones would be generated with the old and incorrect value. This required a work around in the transmitter alignment procedures to have the user enter the Transmitter Configure window to save the values (including the tone amplitudes), since changes in this window **were** correctly written to the transmitter configuration file.

    CRS Build 10.0 has been corrected to write the tone amplitude changes to the transmitter configuration file.

14. **TTR 852: The Save As Function Does Not Work For Listening Areas and Listening Zones** - The CRS GUI includes a *File* menu that allows users to access 5 submenu options. The *Save As* option allows the operator to save the current record under a new name, thereby maintaining the integrity of the originally retrieved record. This option may prove useful in creating new records. For instance, this option could be used in the creation of multiple new Message Types that are very similar. Once all the parameters for the first Message Type are entered and saved, it can be used as a template for the others with the *Save As* option. From most of the GUI windows, the *Save As* option will cause a pop-up window to display with a prompt for a new name that is of variable length. However, prior to Build 10.0, for Listening Areas and Zones, the *Save As* option prompts for a name that is erroneously restricted to 5 characters, rather than 6. This erroneous restriction, therefore, makes it impossible to use the *Save As* function for Listening Areas and Zones.

    The problem is corrected in Build 10.0 by eliminating an incorrect decrement of the maximum length field.

15. **TTR 856: Message Record/Playback Dialog Help Problems** - Clicking on the Help button while in any CRS window forces the Netscape Communicator to display the SOM documentation for that window. Prior to Build 10.0, however, the display for the Weather Message Record/Playback dialog window resulted in the display of an error window which detailed a lock file error in Netscape. Moreover, another Netscape was displayed that listed all the Help files. Upon clicking on the error window OK button, the Record/Playback dialog help window was displayed. Additionally, clicking on the Help button in the Weather Message Text Message Playback dialog window resulted in the display of the Weather Message Correction documentation.

    These problems have been fixed in Build 10.0 so the proper documentation is initially

displayed.

16. **TTR 854: <u>Print Jobs Cannot Be Removed From Print Queue</u>** - The CRS Print Monitor can be invoked from the CRS Utilities menu. Upon doing so, the Print Monitor window will be presented. The currently configured printer and status will be displayed as part of the window title. From this window, the operator may access, select, and submit a job to the printer. Several print management functions also are available to the operator including the ability to remove a job from the print queue via the Remove Job button. However, prior to CRS Build 10.0, pressing this button did not properly remove the print job from the queue.

    This problem has been fixed in Build 10.0 so print jobs can be removed from the queue.